

Journal of Cybersecurity Education, Research and Practice

Volume 2018 | Number 1

Article 4

July 2018

A Case Study in the Implementation of a Human-Centric Higher Education Cybersecurity Program

John W. Coffey

The University of West Florida, jcoffey@uwf.edu


Melanie Haveard

The University of West Florida, mhaveard@uwf.edu

Geissler Golding

The University of West Florida, ggolding@uwf.edu

Follow this and additional works at: <https://digitalcommons.kennesaw.edu/jcerp>

 Part of the [Information Security Commons](#), [Management Information Systems Commons](#), and the [Technology and Innovation Commons](#)

Recommended Citation

Coffey, John W.; Haveard, Melanie; and Golding, Geissler (2018) "A Case Study in the Implementation of a Human-Centric Higher Education Cybersecurity Program," *Journal of Cybersecurity Education, Research and Practice*: Vol. 2018 : No. 1 , Article 4.

Available at: <https://digitalcommons.kennesaw.edu/jcerp/vol2018/iss1/4>

This Article is brought to you for free and open access by DigitalCommons@Kennesaw State University. It has been accepted for inclusion in Journal of Cybersecurity Education, Research and Practice by an authorized editor of DigitalCommons@Kennesaw State University. For more information, please contact digitalcommons@kennesaw.edu.

A Case Study in the Implementation of a Human-Centric Higher Education Cybersecurity Program

Abstract

This article contains a description of the implementation of a comprehensive cyber security program at a regional comprehensive university. The program was designed to create an effective cyber security management infrastructure and to train end users and other categories of security management personnel in data protection and cyber security. This work addresses the impetus for the program, the rather extensive planning and development that went into the program, its implementation, and insights gleaned from the experience. The paper concludes with a summary of the strengths and weaknesses of the initiative.

Keywords

cybersecurity training program, security infrastructure, implementation guidelines, implementation plan, FERPA

INTRODUCTION

The growth of utilization of the Internet and World Wide Web as tools for commerce, collaboration and social interactions continues to be explosive and to some degree, fraught with danger. At the beginning of 2017, one can look back on the multi-million dollar costs associated with cyber breaches of large organizations, the possible role that hacking played in the 2016 U.S. Presidential election, and on countless other smaller losses, both personal and financial, caused by successful cybersecurity exploits.

Accordingly, cybersecurity concerns pervade contemporary discussions of and research pertaining to technology. Institutions of higher education generate and store large quantities of sensitive information that is governed by the Family Educational Rights and Privacy Act (FERPA, 1974). Colleges and universities have many employees who potentially have access to sensitive information, ranging from top-level administrators to faculty, to custodians who might empty a trash can full of student records. Establishing a cybersecurity infrastructure and creating effective training for cybersecurity in colleges and universities is a complex and multi-faceted undertaking.

The remainder of the paper contains a description of the implementation of a human-centered cybersecurity infrastructure and training program at a regional university. After a review of literature pertaining to guidelines for implementing such programs and to human error as a mediating factor in cybersecurity breaches, is a description of the design and implementation of this program. The infrastructure component of the program included creating a cybersecurity policy, creating a comprehensive scheme for tracking and controlling the people who have access to sensitive information, and creation of a cybersecurity management structure.

An extensive training program was also implemented. The training was divided into two parts and encompassed materials pertaining to FERPA (to lay groundwork for the types of information that must be protected), followed by online programmed instructional materials pertaining to ways that data might be compromised and strategies to prevent compromise. The paper concludes with both quantitative and qualitative data on results, and an assessment of strengths and weaknesses of the program.

RELEVANT LITERATURE

The following sections contain literature regarding the many aspects of implementation of a cybersecurity program and the large volume of information that must be distilled in order to formulate and implement a cybersecurity plan. Additionally, literature on the impact of human beings on cybersecurity, a major concern of the program being described in this paper, is described.

Implementing Cybersecurity Programs

Garbars' (2002) work provides insight into how daunting a task it is to create a comprehensive cybersecurity program. He describes guidelines developed at the SANS Institute that integrate a wide variety of federal and state law, federal regulations and guidelines. He lists the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB) the National Security Agency (NSA) and the General Accounting Office (GAO) as just a few of the federal agencies who weigh in on how to implement cybersecurity programs. It is likely that, if he had written the article a few years later, he would have included the Department of Homeland Security (DHS) on the list as well.

To take one example from Garbars' list, the NIST Cybersecurity Framework (2014) provides guidelines for the implementation of a cybersecurity program. The overarching approach in the framework is to identify assets and risks, protect critical assets, detect intrusions, respond to intrusions and recover from incidents, a very broad-stroke framework in which each aspect is complex. Their seven-step process for cybersecurity program implementation includes prioritizing and scoping the undertaking, determining critical assets, determining current organizational cybersecurity strengths and weaknesses, assessing risks, determining cybersecurity goals for the organization, performing gap analysis, and creating and implementing an action plan.

Baker Tilly (2014) provide many broad guidelines regarding the implementation of cybersecurity programs. They describe the need for the classification of data by criticality, implementation of security control management and periodic assessment, breach planning, and decisions either to accept risks associated with data breaches or to transfer risk through a cyber-liability insurance policy. Their recommendations are comprehensive with the exception of a relative lack of focus on preventing end user errors.

Howarth (2014) concludes that organizations that implement strong technological security procedures still often pay insufficient attention to human sources of vulnerability, and strongly advocates for enhanced security training. Armerding (2014) cites a report that indicates that 56% of workers who use the Internet on their jobs receive no security training at all.

The Payment Card Industry (PCI) Security Standards Council (2014) guidelines provide some details on the implementation of training programs. Their framework includes role-based decisions regarding security training rather than a one-size-fits-all training approach. The guidelines mention three basic role categories: all personnel for baseline security training, specialized roles identified by the organization, and management roles that include ongoing responsibilities to promote good security practices. These guidelines do not specify what the specialized roles might be.

The guidelines include mention of various training delivery modes including formal face-to-face programs, online training, use of social media, periodic emails, memos, posters, bulletins, etc. Emphasis is placed on multiple communication modes for security-related messages. PCI also advocates separate training for new hires and people who change jobs within the organization.

McCoy and Fowler (2004) described implementation of a security program at a university. Their program covered password strength issues, workstation security, secure internet and email practices, and FERPA issues. They identified numerous sub-categories of students and faculty as the targeted audiences and attempted to tailor needs to each group. Categories of students included on-campus and off-campus students and the faculty and staff classifications were further sub-divided to include upper level administrators.

Delivery methods included mass emails of security-related materials, articles in various publications and both in-person and online training classes. Interestingly, the issue of whether the training was mandatory or optional was left up to the individual operating units. In their plan for improvement, they stated that they hoped to make mandatory training more pervasive and to incorporate student security training into courses.

Human Factors in Cybersecurity Breaches

IBM's 2016 Cyber Security Intelligence Index (IBM Security Services, 2016) contained many interesting statistics on sources of cybersecurity attacks. The report cited a 5% increase in attacks coming from inside organizations (from 55% to 60%). Of the 55% in 2014, 31.5% were deliberate and 23.5% involved human error. In 2016, the percentage of error-mediated attacks decreased, but still accounted for 15.5% of all security breaches.

IBM's 2014 report (IBM Security Services, 2014) provides some evolutionary perspective. It was based upon nearly 1000 clients in 133 countries and literally billions of events per year. IBM reported that human errors included those made by IT professionals such as improper system security configurations and poor patch management, and those made by end-users such as weak or shared

passwords, loss of devices containing sensitive information, and the single most prevalent: opening an unsafe attachment or accessing an unsafe URL. IBM's ongoing research clearly indicates that the role of end user error in cybersecurity breaches is truly significant and its role as a proximate cause is clearly not decreasing.

Verizon (2013) reports data that corroborates IBM's report. Verizon's report cites the prominent role of poor passwords, claiming that 63% of confirmed data breaches were facilitated by the weak or default passwords, or the theft of passwords. That report goes on to make the claim that 93% of data breaches occur within minutes of the password compromise, but more than 80% of the breaches are not discovered until weeks later. The problem remains significant in 2017, with increasingly sophisticated phishing attacks resulting in more stolen passwords.

Woodhouse (2007) states that organizations need much more than annual awareness training to modify the behaviors of end users. He states that it is critical to cultivate an information security culture with active participation in good security practices. As is the case with so many papers on the subject, Woodhouse's article is long on platitudes but lacking on details regarding how to cultivate such a culture.

Furman, Theofanos, Choong and Stanton (2011) found that end users tend to be aware of and concerned with cybersecurity but they lacked comprehensive understanding of existing threats and of how to protect themselves. When asked to define terms pertaining to security threats such as key logger, spoofing, virus, botnet, etc., participants in Furman's study professed familiarity with the terms but often failed to define the terms correctly. Obviously, without knowing precisely what these threats are, the participants lacked knowledge of how to counter them. While potentially very interesting, the study did not go into participant knowledge of prevention at all.

A very interesting finding discussed by Furman et al., was that the Federal Information Processing Standards (FIPS, 2015), US government standards for civilian employee computer use, address three security concerns:

- confidentiality, the protection of sensitive data from unauthorized people,
- integrity, keeping data from being corrupted or destroyed, and
- availability – ensuring that data can be accessed when needed

Of these three important concerns, survey results revealed that confidentiality was the overriding concern of study participants, and that participants were largely unaware of data integrity and data access issues.

A consequence of the lack of broad understanding of data integrity and access concerns gives rise to a variety of end user errors. End users routinely send sensitive information through email, transport it on jump drives that are easily lost, and place proprietary information on file sharing sites. Point of sale attacks frequently occur and, astonishingly, they are often caused by people who use point of sale machines for unauthorized uses including web surfing and email (Hummer, 2016).

Phishing attacks are still surprisingly successful. Social Engineering including phishing attacks are so widespread and successful that a worldwide working group has formed to try to prevent them (APWG, 2017). These attacks involve tricking people into violating security procedures, opening emails with malware attachments, visiting phishing websites, etc. Personal identification data that was compromised earlier often figures into spear phishing attacks, which are based upon emails that appear to be from trusted sources or businesses with which the target has routine interactions.

Educational institutions have much of the usual data security concerns of other organizations including sensitive employee data, operating revenues and expenses, etc., but they are also governed by FERPA (1974). Understanding and enforcing FERPA regulations is a significant problem for colleges and universities because FERPA regulations are complex. The FERPA website has an FAQ page with more than 200 FAQs, a basic indication of the law's complexity. The various sources of information on the establishment of security programs and the wide variety of human error described here were the backdrop for the establishment of the human-centric security program described in the next sections.

IMPLEMENTING A HUMAN-CENTRIC CYBERSECURITY PROGRAM

The following sections recount the development and implementation of a cybersecurity program aimed at addressing human factors at a regional comprehensive university. It presents details regarding initial motivations for the implementation of the cybersecurity infrastructure, the development of a cybersecurity policy, implementation of a cybersecurity management structure including implementation of a system to track data access of employees, and the implementation of a broad training program.

Initial Motivations for the Program

At least three separate events gave impetus to the creation of the program. During 2015, the university completed a large-scale migration to a new student record management system. The migration triggered a system security audit that yielded a list of findings that was significantly more extensive than expected. Separately, evidence was found that led to concerns regarding faculty and staff understanding of FERPA regulations and constraints, particularly with regard to a variety of poor security practices.

Also in 2015, the University's Computer Science department sought Center for Academic Excellence (CAE) designation for its cybersecurity program. One of the requirements to attain this designation was evidence of a formalized security program at the institution. Finally, the University had several ransomware attacks on network drives that, while ultimately resolved without paying any ransoms, consumed significant time and resources.

The confluence of these events led to the perception of a need to develop a cybersecurity improvement program through an integrated approach that would address all the problems simultaneously. Planning commenced in late fall, 2015 with the goal of implementing rather sweeping changes that would significantly improve the security status of the university during 2016.

The Scope of the Program

While access issues pertaining to the new student record system were the initial focus and a major driver of the initiative, the decision was made to adopt a comprehensive, top-down planning approach. While an incremental approach of training those accessing the new student system and working out from there was attractive because it would quickly address security issues on that important system, a more comprehensive approach to all facets of the problem was adopted.

It was thought that starting from a top-down, overarching view of the totality of the problem enabled an initial scoping that would yield better results than would have occurred from a bottom-up, piecemeal approach. Overall, this decision meant simultaneously developing a security policy statement, a system to centralize monitoring of employee access to sensitive information, a security management structure and accompanying responsibility designations, and a broad training program for all employees.

Since one of the most important findings of the audit of the student record system was the lack of a security awareness-training program, and such a program was a basic requirement for the CAE designation, the design of a security awareness program became a high priority. At the same time, other important considerations including the development of the security management structure

and a means to identify and control access among the end user cohort of the university were addressed.

The Chief Technology Officer of the university originated the concept of a “Knowledge Worker” certification for the training component. The decision was made that since all faculty, staff and graduate students potentially have access to sensitive information, all should be trained. Staff and Graduate students could be required to take the training, but faculty activities are legislated by a Collective Bargaining Agreement (CBA). The CBA precludes mandatory training for faculty, a consideration that required a work-around. Ultimately, it was decided to give incentives to faculty to take the training by withholding computer upgrades for those who did not complete it.

Training in particulars of FERPA was key. FERPA regulations differentiate between protected student information and information that can be freely disseminated. The law is somewhat complex, not always intuitive (for instance, an instructor cannot share information regarding a student’s performance with his or her parents if the student has attained majority age), and it has numerous exemptions that require interpretation. Although protecting FERPA-regulated data was a major concern, the broader issue of protecting all university hardware, software, and data assets was deemed in-scope for the program.

Program Development

The security audit revealed a critical deficiency, the lack of an Information Security and Privacy Policy. The Information Technology Services (ITS) department created a policy by tailoring a template policy obtained from another university in the state university system to the university’s needs. Creation of the policy was valuable in determining the scope of changes that needed to be made.

Another important need that was identified by the security audit was the ability to track and control systems to which the members of the user community have access. Several aspects of this problem were identified including removing access when employment ends, modifying accesses when employees change positions within the university, and knowing which accesses to grant to replacement employees when departing employees are replaced. In order to address this requirement, the decision was made to develop a dashboard in-house that would centralize general employee information, and specifically, information regarding data to which each employee has access. The system, named Security Certifications and Other info On a Person (SCOOP) was developed in-house during 2016.

An important planning issue regarding the security awareness-training component was a buy or build decision regarding the training materials. Given the limited window for implementation of the program, the decision was made to license training materials. By good chance, a company that provides online certification training had been soliciting business from the university for some time. A second company was briefly considered, but the decision was quickly made to have the first company provide the training materials.

The need to create a formalized security management infrastructure was a critical need identified in the security audit. The university has systems administrators at the university level (as members of the Information Technology Services department) and a patchwork of systems administrators, typically working at the College level (local service providers – LSPs). Many of these people were de-facto in charge of security concerns, but their security-related responsibilities and reporting structure were not formalized.

The position of Departmental Information Security Representative (DISRep) was created. DISReps are responsible for maintaining current lists of people within departments and letting Information Technology Services know when new people arrive or current employees leave or change jobs. They also manage access group memberships and they are required to ensure that people under their purview complete required training. Additionally, Security Managers are being designated for each system at the university. Security Managers are tasked with updating user access assignments for all users they manage.

The General Training Program

The general training initiative was created for all faculty and staff and it was comprised of several parts. Training was delivered online and included the following components:

- FERPA basics
- Checkpoint: Data Security and Privacy
- Knowledge Worker Skills Assessment
- Statement of Understanding Regarding Confidentiality

FERPA basics introduced the trainee to basic FERPA definitions, students who fall under FERPA regulations, definitions of directory (public) and private information, exceptions to FERPA privacy regulations and students' rights with respect to the law.

The Data Security and Privacy course started with information regarding the data security problem, risky end user behaviors, the concept of phishing attacks and the overall scope of the problem. It continued with a detailed account of the types of sensitive information end users might have, and the many ways that

accidental disclosure might occur. It continued with a detailed account of the types of attacks on people that occur: phishing emails, spear phishing attacks, pharming, watering hole attacks and so-called “hyperlink hoaxes.” The course continued with information regarding the protection of sensitive data on mobile devices, wireless network security, using cloud storage safely, creating strong passwords and encrypting sensitive data. The security tutorial concluded with the importance of reporting breaches. The materials, while quite comprehensive, were not overly time-consuming to complete.

Although the FERPA and Data Security and Privacy courses had associated quizzes, a separate quiz entitled Knowledge Worker Skills Assessment was also included. Although ostensibly a quiz, it was multiple choice and if the trainee selected an incorrect answer, additional tries were permitted until the correct answer was chosen. As such, it was essentially a chance to reinforce the ideas that had been presented in the first two sections. Finally, trainees had to sign a certification acknowledging that they are responsible for any critical data to which they had access.

Specialized Training and “Grandfathering”

As stated, training was mandatory for staff, but it could not be enforced for faculty. Consequently, a policy of “grandfathering” faculty who did not complete the training had to be implemented. The policy allowed them to continue to access sensitive data. Nine percent of faculty were “grandfathered” in. Specialized training was also provided for DISReps, and is planned for Security Managers. The nature of the Security Manager training is still being determined at the time of this writing.

RESULTS OF THE INITIATIVE

This section contains a summary of the results of the initiative. It briefly recounts the accomplishments regarding the development of a security infrastructure and then focuses on the outcomes of the training program. In the quantitative section, statistics regarding program participation and completion are presented. Additionally, observations made by a College-level training coordinator who had the responsibility to foster participation in the program are summarized.

The Security Infrastructure

In the course of a year, the university was able to go from having no security policy, no security management infrastructure, no centralized means of tracking employee access to systems, and no security-training program, to having all of these capabilities in place. The ability to find a relevant mature security policy

statement from a sister university was invaluable in the efficient formulation of the policy, as was the use of a pre-packaged security awareness tutorial.

The development of a security management infrastructure was critical and not without its difficulties. ITS employees and local service providers, all of whom already had quite busy professional lives, had to take on additional responsibilities and reporting requirements. Specialized training was offered for the DISReps. Training programs for the security managers are undergoing development and, as of this writing, have not yet been offered.

Implementation of the SCOOP system was completed during the 2016 calendar year and the system is up and running. This system plays a critical role in the control of access to sensitive information. It plays an additional helpful role by centralizing employee data.

Perhaps the most visible accomplishment of this initiative was the successful implementation of the general training program. It was a difficult challenge because of several factors including the lack of authority to require faculty to take the training, the problem of adjunct professors who might not be registered to teach in the time window that training was offered, and low technical skills among some of the employees. The next sections provide some data on training outcomes.

Quantitative Training Results

The training window for the initial round of general training was from November 1, 2016 to the end of January, 2017. Table 1 (next page) contains information pertaining to participation in the program. As can be seen in Table 1, more than 2000 employees were slated to take the training and 82% completed it successfully. The university is divided into 147 different academic and non-academic operating units, and more than half of the units had 100% training completion by their cohorts. More than 91% of in-unit faculty completed the training.

Observations from a Training Coordinator

An Associate Dean of one of the University's Colleges was tasked with overseeing the program for his College. His main responsibility was to foster participation in the training. Since the training could not be required, he was tasked with motivating the faculty to do the work. He did this by sending several emails to department chairs, including an estimated 4-5 in the last month of the program. Additionally, he used word of mouth to spread awareness of the training. He was also tasked with overseeing the DISReps and he was able to coordinate with them to encourage faculty and staff to complete the training.

Table 1: Statistics pertaining to training completion at the end of the initial program (January 31, 2017).

Category	Count or Percentage
Individual Trainees	
Total trainees	2132
Total Trainees completing the program	1753
Percentage of total trainees completing the program	82%
Academic Divisions/Units	
Total divisions/units with personnel who took training	147
Total divisions/units with 100% completion	76
Percentage of Units with 100% completion	52%
In-Unit Faculty	
Total In-Unit Faculty	344
Total In-Unit Faculty completing the program	313
Percentage of In-Unit Faculty completing the program	91%

He did not receive a lot of formal feedback on the quality of the program. Anecdotally, he stated that the program was generally deemed to be of acceptable quality and worthwhile. Feedback he received indicated that some deemed the materials too elementary and others thought them too advanced. Some had taken FERPA training previously and thought it unnecessary.

A certain amount of complaint was noted anecdotally. Some technical issues with the online training were noted; for instance, materials only worked properly on Windows machines running the Chrome browser. Twenty five percent of the personnel in the College used MacOS, which caused some difficulties with the materials.

The Training Coordinator had a plan to get Adjuncts pre-certified to teach, but he encountered a problem with not being able to get prospective adjuncts access to the training materials until they had a University userid and password. University userids and passwords are not assigned until adjuncts are assigned courses. Issues such as these are destined to arise in any large-scale training program encompassing thousands of employees. Overall, the training effort as implemented would be deemed a success by any reasonable measure.

CONCLUSIONS

The undertaking to implement a comprehensive, human-centric security program was multi-faceted, time-consuming, and ambitious. Technological issues such as system administrator training and standard security operations such as firewall and patch maintenance went on in parallel and are not reported here. In the course of a year, the university succeeded in implementing a comprehensive security policy, a system to track employee access, a security management hierarchy, and a large-scale security-training program. The encompassing, top-down approach to the planning and implementation of the program worked well. This approach contrasted sharply with an incremental approach that might have been adopted. The training program was successful in terms of participation considering that faculty could not be required to participate. Most employees saw only a small part of the overall effort. While some of the training is still in the planning phase and students were not included in the current program, the implementation of the program has been deemed a significant success.

REFERENCES

- Addae, J., Radenkovic, X.S., & Towey, D. (2016). An Extended Perspective on Cybersecurity Education. The 2016 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE). pp 367-369. Bangkok, Thailand.
- APWG. (2017). APWG: Unifying the Global Response to Cybercrime. Online, Available: <http://www.antiphishing.org/>
- Armerdeing, T. (2014). Security training is lacking: Here are tips on how to do it better. Online, Available: <http://www.csoonline.com/article/2362793/security-leadership/security-training-is-lacking-here-are-tips-on-how-to-do-it-better.html>.
- Baker Tilly (2014). Implementing an effective cybersecurity management program. Online Available: <http://bakertilly.com/insights/implementing-an-effective-cybersecurity-management-program/>
- FERPA. (1974). Family Educational Rights and Privacy Act (FERPA) Online, Available: <https://ed.gov/policy/gen/guid/fpco/ferpa/index.html>
- FIPS. (2015). Federal Information Processing Standateds Publications. Online Available: <http://src.nist.gov/publications/PubsFIPS.html>

- Furnam, S., Thelfanos, M.F., Choong, Y-Y., & Stanton, B. (2011). Basing Cybersecurity Training on User Perceptions. *IEEE Security and Privacy* 10(2). pp 40 – 49.
DOI: 10.1109/MSP.2011.180
- Glaser, A. (2016). Here's What We Know about Russia and the DNC Hack.
<https://www.wired.com/2016/07/heres-know-russia-dnc-hack/>
- Garbars, K. (2002). Implementing an Effective IT Security Program. SANS Institute. Online
Available: <https://www.sans.org/reading-room/whitepapers/bestprac/implementing-effective-security-program-80>.
- Grunzweig, J. (2015). Understanding and Preventing Point of Sale Attacks. Online. Available:
<http://researchcenter.paloaltonetworks.com/2015/10/understanding-and-preventing-point-of-sale-attacks/>
- Howarth, F. (2014). The Role of Human Error in Successful Security Attacks. Online. Available:
<https://securityintelligence.com/the-role-of-human-error-in-successful-security-attacks/>
- Hummer, L. (2016). Security Starts with People: Three Steps to Build a Strong Insider Threat Protection Program Online, Available: <https://securityintelligence.com/security-starts-with-people-three-steps-to-build-a-strong-insider-threat-protection-program/>
- IBM Security Services. (2014). Cybersecurity Intelligence Index. Online.
Available:https://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf
- IBM Security Services. (2016). Cybersecurity Intelligence Index. Online. Available:
https://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf
- McCoy, C. & Fowler, R. T. (2004). You Are the Key to Security: Establishing a Successful Security Awareness Program. *Proceedings of SIGUCCS'04*. 2004. pp 346-349. ACM 1-58113-869-5/04/0010.
- NIST. (2014). Framework for Improving Critical Infrastructure Cybersecurity. Online. Available:
<https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>
- PCI Security Standards Council. (2014). Best Practices for Implementing a Security Awareness Program.
https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf.
- Verizon. (2013). 2013 Data Breach Investigations Report. Online, available:
http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf
- Woodhouse, S. (2007). Information Security: End User Behavior and Corporate Culture. *Proceedings of the Seventh International Conference on Computer and Information Technology*. IEEE. DOI 10.1109/CIT.2007.186. pp 767-772.